

Códigos Secretos: otra forma de aplicar las matrices en Bachillerato (16-18)

Julián Baena Ruiz

Tras una breve introducción para hacer referencia a distintos tipos de códigos secretos, el artículo estudia con detalle, esquemáticamente y mediante ejemplos, los códigos matriciales. Se expone, además, una forma de automatizar dichos códigos en el aula, mediante un programa escrito en dBASE III Plus. La parte final consta de unas preguntas sobre sus posibilidades didácticas.

Objetivo

Se quiere presentar la criptografía como un campo de aplicación del cálculo matricial y un contexto para conectar dicho estudio con la programación de ordenadores. Las ideas expuestas pretenden ser útiles a profesores que busquen enfoques distintos de esta parte del álgebra lineal y, para ello, estén dispuestos a utilizar ordenadores.

Introducción

Criptografía significa arte de escribir con una clave secreta. Nos referiremos en adelante a esta clave con el nombre de código.

Algunos códigos secretos, a los que llamaremos elementales, se basan en la sustitución de cada carácter por un determinado símbolo. Por ejemplo si la letra A se sustituye por el signo +, la M por ?, O por % la palabra "AMO" se codifica: "+?%". Un ejemplo de ellos aparece en el cuento de Edgar Allan Poe¹ "El escarabajo de oro" [1]; aquí se explican, razonadamente, estrategias que conducen a descifrar un criptograma. Todos los códigos elementales son equiva-

lentes y fáciles de descifrar comparando las frecuencias con que aparecen los símbolos en el texto codificado, con las frecuencias de aparición de los caracteres en el idioma usado para escribir. Algunos autores (profesores) han propuesto actividades para clase, usando códigos de este tipo [2]; en ellas se deja claro lo fácil que resulta descubrir un código elemental utilizando la Estadística.

En los últimos años, y debido al interés creciente de proteger la información en las comunicaciones, la criptografía ha logrado grandes progresos a partir de códigos secretos más avanzados, cuya descripción sería imposible sin conocimientos de álgebra [3]. Entre ellos podemos citar los que usan vectores y matrices [4] (para nosotros matriciales), basados en las ideas de Hill [5], de los que nos vamos a ocupar a continuación, y otros, que se estudian a partir de resultados de la Teoría de Números [6], iniciados con trabajos de Diffie y Hellman donde se trata la criptografía en términos matemáticos y un "sistema criptográfico" es considerado como una "familia uniparamétrica de transformaciones invertibles" [7] (pág. 646).

Códigos matriciales

Tratando de evitar el abuso de formalismos, que puedan aburrir a los menos iniciados, la exposición de esta sección se basa en casos particulares; así el lector podrá dar, a medida que avanzamos, un tratamiento más general a todo lo que hay escrito.

Comenzamos definiendo un conjunto S formado por todos los signos disponibles para escribir los textos que después se codificarán. Este conjunto, por comodidad, lo consideramos compuesto por las letras del alfabeto castellano, (excepto la ll y la ch) el espacio (que representaremos en esta sección mediante "-"), el signo de interrogación "?" y el punto ".". Nuestro conjunto S tiene 30 elementos.

$$S = \left\{ \begin{array}{l} A, B, C, D, E, F, G, H, I, J, K, L, M, N, \bar{N} \\ O, P, Q, R, S, T, U, V, W, X, Y, Z, \dots, -, ? \end{array} \right\}$$

Definición: Llamamos S-mensaje a una secuencia de caracteres del conjunto S, que escribiremos siempre entre comillas.

Por ejemplo:

M = "HOLA-BUENAS-NOCHES"

¹ Poe fue un reconocido criptoanalista.

Tomar matriz $\begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}$ más fácil $\begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 29 \\ 27 & 2 \end{pmatrix}$ Inversa

$$\text{Hacer prueba } \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 2 & 29 \\ 27 & 2 \end{pmatrix} = \begin{pmatrix} 31 & 60 \\ 60 & 41 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Mensaje más corto:

CABE — (3,1) (2,5) 3125

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z . ? -

$$\begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 7 \\ 11 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 2 \\ 5 \end{pmatrix} = \begin{pmatrix} 9 \\ 16 \end{pmatrix}$$

CABE → GKIO

$$\begin{pmatrix} 2 & 29 \\ 27 & 2 \end{pmatrix} \begin{pmatrix} 7 \\ 11 \end{pmatrix} = \begin{pmatrix} 333 \\ 211 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix} - CA$$

$$\begin{pmatrix} 2 & 29 \\ 27 & 2 \end{pmatrix} \begin{pmatrix} 9 \\ 16 \end{pmatrix} = \begin{pmatrix} 482 \\ 864 \end{pmatrix} = \begin{pmatrix} 2 \\ 5 \end{pmatrix} - BE$$

Establecemos, a continuación, una correspondencia 1-1, f , de S en Z_{30} (conjunto de los enteros módulo 30). Por ejemplo elegimos $f(x)=n$, donde n es la clase del número que ocupa x en el orden dado anteriormente. De esta forma tenemos identificado S con Z_{30} .

1. Pasos a seguir para la codificación

(con un ejemplo 2×2)

Vamos a codificar el mensaje M del ejemplo anterior. Para ello seguiremos los siguientes pasos:

1.1. Elegimos una matriz 2×2 invertible sobre Z_{30} por ejemplo:

$$A = \begin{pmatrix} 8 & 1 \\ 1 & 4 \end{pmatrix}$$

Esta matriz determina unívocamente el código y su dimensión 2×2 da nombre a los códigos de este tipo.

1.2. Pasamos, mediante la aplicación f , del mensaje a un conjunto ordenado de números (imágenes de los caracteres que aparecen en M). En nuestro caso:

8 16 12 1 0 2 22 5 14 1 20 0 14 16 3 8 5 20

1.3. A partir de este conjunto definimos, ordenadamente, pares de números como se hace a continuación:

(8,16) (12,1) (0,2) (22,5) (14,1) (20,0) (14,16) (3,8) (5,20)²

1.4. Multiplicamos por la matriz A , cada uno de los pares anteriores y resulta:

(20,12) (7,16) (2,8) (1,12) (23,18) (10,20) (8,18) (2,5) (0,25)

1.5. Obtenemos una nueva secuencia numérica:

20 12 7 16 2 8 1 12 23 18 10 20 8 18 2 5 0 25

1.6. Aplicando la inversa de f , conseguimos el mensaje codificado:

$M' = \text{"SLGOBHALUQJSHQBE-X"}$

Llamaremos a M' S-mensaje codificado por A o imagen de M mediante A , y escribiremos:

$$M' = A(M)$$

2. Pasos a seguir para decodificar un mensaje

Es un proceso análogo al anterior. Consiste en hacer lo mismo que en 1. partiendo del mensaje M' y eligiendo, en el primer punto 1.1, como matriz, la inversa de A (que llamaremos B):

$$B = \begin{pmatrix} 4 & 29 \\ 29 & 8 \end{pmatrix} \quad \begin{matrix} -2 \\ 1 \end{matrix} \quad (*)$$

No es necesario efectuar cálculos para asegurar que, el S-mensaje codificado de M' , mediante B , es M .

3. Generalización

Es imprescindible definir con precisión el conjunto S de símbolos que se utilizarán para escribir, y su cardinal, k , nos conducirá a trabajar en el anillo Z_k de los enteros módulo k .

Como se indicó antes, el código viene determinado unívocamente por la matriz invertible A (definida sobre

Z_k). Si A es cuadrada de orden n , en el punto 1.3. formaremos n -uplas y completaremos la última con los ceros que sean necesarios (en el caso de que la longitud del S-mensaje de partida no sea múltiplo de n).

Podemos, incluso codificar usando matrices no cuadradas $m \times n$ procurando que para A (la que codifica) exista una matriz B de orden $n \times m$ tal que el producto $A \cdot B$ sea la matriz I (identidad) $m \times m$; hablándose así, según la matriz, de códigos 2×2 , 3×3 , 4×5 , etc.

Conviene destacar que un código 1×1 , definido por unidad de Z_k , será a todos los efectos un código elemental, pues lo único que introduce es una permutación en el orden de los caracteres.

² Se colocaría un cero en el último par, si el mensaje de partida tuviese un número impar de caracteres.

³ Del IB "Mediterráneo" de Salobreña (Granada)

$$(*) \quad \text{Adj } A = \begin{pmatrix} 4 & 29 \\ 29 & 8 \end{pmatrix} \quad |A| = 32 - 1 = 31 = 1(30)$$

$$A_{11} = 4 \quad A_{12} = -1 = 29(30)$$

$$A_{21} = 29 \quad A_{22} = 8 \quad \text{Luego } A^{-1} = \begin{pmatrix} 4 & 29 \\ 29 & 8 \end{pmatrix}$$